





# ANONYMOUS MESSAGE TRANSMISSION SYSTEM AND VOTING SYSTEM

**Patent number:** JP8263575  
**Publication date:** 1996-10-11  
**Inventor:** SAKO KAZUE; JIYOSUFU JIEI KIRIAN  
**Applicant:** NEC CORP  
**Classification:**  
 - international: G06F19/00; G09C1/00  
 - european:  
**Application number:** JP19950335493 19951222  
**Priority number(s):**

Also published as:

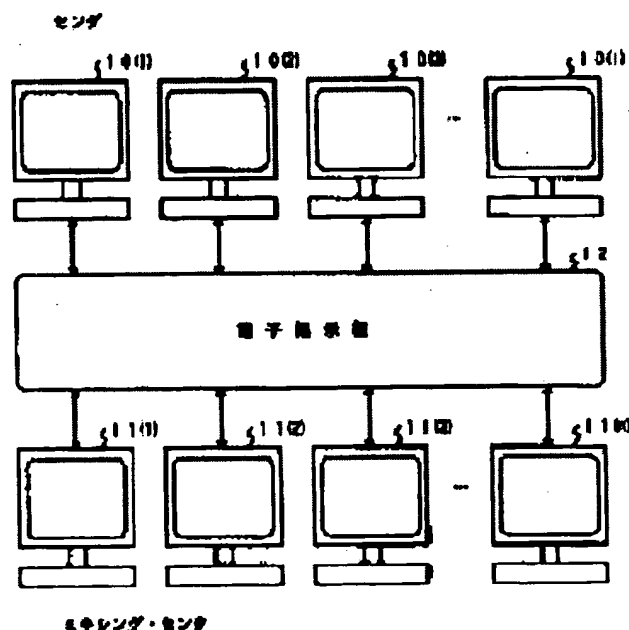
 EP0723349 (A2)  
 US5682430 (A1)  
 EP0723349 (A3)  
 EP0723349 (B1)

Report a data error here

## Abstract of JP8263575

**PURPOSE:** To enable an outside observer to verify whether or not an election is carried out actually correctly by sequentially processing ciphered messages from senders at a mixing center and outputting a group of messages which are ciphered in random order wherein they can not be traced finally.

**CONSTITUTION:** Voters vote through senders 10(1), 10(2)... equipped with arithmetic means, suitably, personal computers. Similarly, respective mixing centers 11(1), 11(2)... are equipped with arithmetic means, suitably, personal computer, work stations, etc. Then the senders 10(1), 10(2)... report voter's ciphered messages firstly to an electronic bulletin board 12 or other openly usable message means. A center 11(i) processes respective messages reported by a preceeding center 11(i-1) and makes the results in shuffled order. This is carried out until the final center 11(n) makes the totalization result of the voting open to the public.



Data supplied from the esp@cenet database - Patent Abstracts of Japan

(19)日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-263575

(43)公開日 平成8年(1996)10月11日

(51)Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 19/00			G 0 6 F 15/28	B
G 0 9 C 1/00	6 6 0	7259-5 J	G 0 9 C 1/00	6 6 0 Z

審査請求 有 請求項の数34 O L 外国語出願 (全 32 頁)

(21)出願番号 特願平7-335493

(22)出願日 平成7年(1995)12月22日

(31)優先権主張番号 08/376568

(32)優先日 1995年1月23日

(33)優先権主張国 米国 (US)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 佐古 和恵

東京都港区五丁目7番1号 日本電気株式会社内

(72)発明者 ジョセフ ジェイ. キリアン

アメリカ合衆国, ニュージャージー

08550, プリンストン ジャンクション,

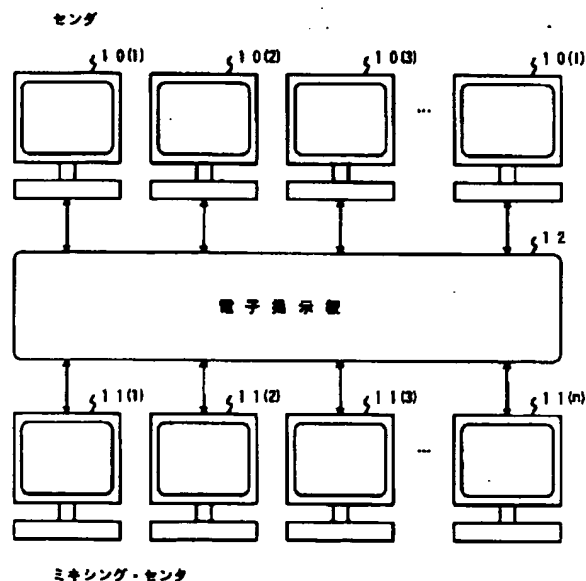
リード ドライブ ソース 18

(74)代理人 弁理士 後藤 洋介 (外2名)

(54)【発明の名称】 匿名メッセージ伝送方式および投票方式

## (57)【要約】

【解決手段】 数論的アルゴリズムは、匿名メッセージ伝送および電子投票を与える。投票者またはセンダは、暗号化された投票またはメッセージを送る。投票またはメッセージは、n個のセンダによって処理され、不正行為を防止し、投票が正当であることを証明する。いかなる利害関係人も、各投票が適正に計算されたことを検証することができる。この発明は、電子掲示板にアクセスできる現世代のパーソナル・コンピュータによって実現できる。



## 【特許請求の範囲】

【請求項1】 複数のミキシング・センタを用いることによって、複数のセンダから匿名メッセージを送送する方法において、

(a) センダ $S_1, S_2, \dots, S_i$  およびミキシング・センタ $C_1, C_2, \dots, C_i$  に対して公開される定数を選択するステップと、

(b) 各センダ $S_i$  が、公開される暗号化メッセージを構成するステップと、

(c) 第1のミキシング・センタ $C_1$  が、各センダ $S_i$  からの公開メッセージを処理し、処理したメッセージを次のミキシング・センタによる使用のために公開するステップと、

(d) 各ミキシング・センタ $C_2 \sim C_{i-1}$  が、前のミキシング・センタからの処理されたメッセージを逐次的に処理し、逐次的に処理されたメッセージを、次のミキシング・センタによる使用のために公開するステップと、

(e) 最終のミキシング・センタ $C_i$  が、前のミキシング・センタ $C_{i-1}$  からのメッセージを処理し、結果を公開するステップと、

(f) 各ミキシング・センタが、その処理の正当性を証明し、そのブルーフを公開するステップと、

(g) チャンネル・チェッカが、必要に応じて、公開されたメッセージから実行の正しさを検証するステップとを含む、匿名メッセージ伝送方法。

【請求項2】 請求項1記載の匿名メッセージ伝送方法において、前記ステップ(c), (d), (e)はさらに、

(h) 各ミキシング・センタに秘密鍵を備えるステップと、

(i) 前記処理が、各ミキシング・センタの秘密鍵を用いるステップとを含む、匿名メッセージ伝送方法。

【請求項3】 請求項2記載の匿名メッセージ伝送方法において、前記ミキシング・センタの証明ステップは、アルゴリズム $prove-DECRYPT$ の実行を含む、匿名メッセージ伝送方法。

【請求項4】 請求項3記載の匿名メッセージ伝送方法において、前記アルゴリズム $prove-DECRYPT$ の実行は、多数のメッセージに対して一緒に実行される、匿名メッセージ伝送方法。

【請求項5】 請求項2記載の匿名メッセージ伝送方法において、前記証明ステップは、 $Fiat-Shamir$ 法を適用することを含む、匿名メッセージ伝送方法。

【請求項6】 請求項2記載の匿名メッセージ伝送方法において、

(j) メッセージをシャッフルするステップをさらに含む、匿名メッセージ伝送方法。

【請求項7】 請求項6記載の匿名メッセージ伝送方法において、前記証明ステップは、アルゴリズム $prove-SHUFFLE$ の実行を含む、匿名メッセージ伝送

方法。

【請求項8】 請求項1記載の匿名メッセージ伝送方法において、前記ステップ(c), (d), (e)は、メッセージをシャッフルするステップをさらに含む、匿名メッセージ伝送方法。

【請求項9】 請求項8記載の匿名メッセージ伝送方法において、最終のミキシング・センタ $C_i$  が結果を通知した後に、各ミキシング・センタは、前記結果を用いてアルゴリズム $prove-DECRYPT$ を実行し、ステップ(d)および(e)を繰返すことを含む、匿名メッセージ伝送方法。

【請求項10】 請求項8記載の匿名メッセージ伝送方法において、各ミキシング・センタは秘密鍵を備え、最終のミキシング・センタ $C_i$  が結果を通知した後に、各ミキシング・センタは、その各秘密鍵および前記結果を用いて前記処理を実行し、ステップ(d)および(e)を繰返すことを含む、匿名メッセージ伝送方法。

【請求項11】 請求項8記載の匿名メッセージ伝送方法において、前記証明ステップは、アルゴリズム $prove-SHUFFLE$ の実行することを含む、匿名メッセージ伝送方法。

【請求項12】 請求項11記載の匿名メッセージ伝送方法において、前記証明ステップに、 $Fiat-Shamir$ 法を適用することを含む、匿名メッセージ伝送方法。

【請求項13】 請求項8記載の匿名メッセージ伝送方法において、前記証明ステップに、 $Fiat-Shamir$ 法を適用することを含む、匿名メッセージ伝送方法。

【請求項14】 請求項1記載の匿名メッセージ伝送方法において、前記証明ステップに、 $Fiat-Shamir$ 法を適用することを含む、匿名メッセージ伝送方法。

【請求項15】 請求項1記載の匿名メッセージ伝送方法において、前記ステップ(b)で、各センダ $S_i$  は、その暗号化メッセージを本質的に同時に公開することを含む、匿名メッセージ伝送方法。

【請求項16】 請求項1記載の匿名メッセージ伝送方法において、ステップ(b)で、各センダ $S_i$  は、前記第1のミキシング・センタ $C_1$  の鍵を用いて暗号化メッセージを構成し、前記暗号化メッセージは、各センダ $S_i$  の署名を含む、匿名メッセージ伝送方法。

【請求項17】 請求項1記載の匿名メッセージ伝送方法において、ステップ(b)で、各センダ $S_i$  は暗号化メッセージを構成し、この暗号化メッセージは、前記第1のミキシング・センタ $C_1$  が各暗号化メッセージを受信した後に、公開されることを含む、匿名メッセージ伝送方法。

【請求項18】 請求項1記載の匿名メッセージ伝送方法において、前記第1のミキシング・センタ $C_1$  は、適

3

正なメッセージのみを処理し、および各センダからただ1つのメッセージを処理することを含む、匿名メッセージ伝送方法。

【請求項19】 請求項18記載の匿名メッセージ伝送方法において、前記センダは、投票者であり、前記メッセージは投票文である、匿名メッセージ伝送方法。

【請求項20】 請求項19記載の匿名メッセージ伝送方法において、前記最終ミキシング・センタC。の前記処理に投票結果を計算することを含む、匿名メッセージ伝送方法。

【請求項21】 匿名メッセージを伝送する装置において、

定数を記載する掲示板と、

複数のセンダ $S_1, S_2, \dots, S_i$ とを備え、各センダ $S_i$ は、前記定数を用いて暗号化メッセージを構成し、前記暗号化メッセージを前記掲示板に通知し、

複数のミキシング・センタ $C_1, C_2, \dots, C_i$ を備え、第1のミキシング・センタ $C_1$ は、前記定数を用いて各センダからの通知メッセージを処理して、処理されたメッセージを、次のミキシング・センタによる使用のために前記掲示板に通知し、各ミキシング・センタ $C_2 \sim C_{i-1}$ は、前記定数を用いて前のミキシング・センタからの処理されたメッセージを逐次的に処理し、さらに処理されたメッセージを、次のミキシング・センタによる使用のために前記掲示板に通知し、最終のミキシング・センタ $C_i$ が、前記定数を用いて前のミキシング・センタ $C_{i-1}$ からのメッセージを処理し、結果を前記掲示板に通知し、

各ミキシング・センタに関連し、各ミキシング・センタの処理の正当性を証明し、そのブルーフを前記掲示板に通知する手段と、

通知されたメッセージから実行の正しさを検証するチャンネル・チェック手段とを備える匿名メッセージ伝送装置。

【請求項22】 請求項21記載の匿名メッセージ伝送装置において、各ミキシング・センタに関連し、メッセージの処理のために前記各ミキシング・センタが秘密鍵を保持する秘密鍵保持手段をさらに備える、匿名メッセージ伝送装置。

【請求項23】 請求項22記載の匿名メッセージ伝送装置において、前記ミキシング・センタは、アルゴリズム $\text{prove-DECRYPT}$ を実行することによって、メッセージを処理する、匿名メッセージ伝送装置。

【請求項24】 請求項23記載の匿名メッセージ伝送装置において、各ミキシング・センタに関連する前記各手段は、アルゴリズム $\text{prove-DECRYPT}$ を実行する、匿名メッセージ伝送装置。

【請求項25】 請求項24記載の匿名メッセージ伝送装置において、各ミキシング・センタに関連する各手段は、多数のメッセージに対しアルゴリズム $\text{prove-}$

4

$\text{DECRYPT}$ を実行する、匿名メッセージ伝送装置。

【請求項26】 請求項21記載の匿名メッセージ伝送装置において、前記ミキシング・センタは、メッセージをシャッフルすることによってメッセージを処理する、匿名メッセージ伝送装置。

【請求項27】 請求項26記載の匿名メッセージ伝送装置において、前記ミキシング・センタは、アルゴリズム $\text{prove-SHUFFLE}$ を実行することによってメッセージを処理する、匿名メッセージ伝送装置。

10 【請求項28】 請求項26記載の匿名メッセージ伝送装置において、各ミキシング・センタに関連した前記各手段は、アルゴリズム $\text{prove-SHUFFLE}$ を実行する、匿名メッセージ伝送装置。

【請求項29】 請求項21記載の匿名メッセージ伝送装置において、各センダ $S_i$ は、その暗号化メッセージを、前記掲示板にほぼ同時に通知する、匿名メッセージ伝送装置。

【請求項30】 請求項22記載の匿名メッセージ伝送装置において、各センダ $S_i$ は、前記第1のミキシング・センタ $C_1$ の前記秘密鍵を用いて暗号化メッセージを構成し、前記暗号化メッセージは、各センダ $S_i$ の署名を含む、匿名メッセージ伝送装置。

【請求項31】 請求項21記載の匿名メッセージ伝送装置において、各センダは、暗号化メッセージを構成し、この暗号化メッセージは、前記第1のミキシング・センタ $C_1$ が各暗号化メッセージを受信した後に、公開される、匿名メッセージ伝送装置。

【請求項32】 請求項21記載の匿名メッセージ伝送装置において、前記第1のミキシング・センタ $C_1$ は、適正なメッセージのみを処理し、および各センダからただ1つのメッセージを処理する、匿名メッセージ伝送装置。

【請求項33】 請求項32記載の匿名メッセージ伝送装置において、前記センダは、投票者であり、前記メッセージは投票文である、匿名メッセージ伝送装置。

【請求項34】 請求項33記載の匿名メッセージ伝送装置において、前記結果は投票結果を有する、匿名メッセージ伝送装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、匿名メッセージ伝送に関し、特に、無記名電子投票のための数論的方法および装置に関するものである。

【0002】

【発明の背景】無記名電子投票は、秘密マルチ・パーティ(multi-party)計算の最も重要な応用の1つである。この無記名電子投票について多くの研究がなされているにも拘らず、理論的または実証的な領域のいずれにおいても、完全な解決法は発見されていない。

50 秘密マルチ・パーティ・プロトコルに対する一般的な解

5

決法は、選挙の必要なセキュリティ特性のすべてを実現することができない。

【0003】かなり異なるセキュリティ特性を有する、より実効的な多くの投票プロトコルが、提案されている。匿名チャンネル／ミキサに基づく方式は、それらの優れた効率および許容される投票の任意性により、非常に一般的になってきた。

【0004】混合ネット (Mix-net) 匿名チャンネルは、文献 "Untraceable Electronic Mail, Return Address, and Digital Pseudonyms" in Communication of the ACM, 1981, pp. 84~88にD. Chaumによって最初に提案された。続いて、この基本技術に基づいて多くの投票方式が提案されている。例えば、A. Fujiokaらにより文献 "A Practical Secret Voting Scheme for Large Scale Elections", in Advances in Cryptology - Auscrypt' 92, 1992, pp. 244~251に、また、C. Parkらにより文献 "All/Nothing Election Scheme and Anonymous Channel" in Advances in Cryptology, Eurocrypt' 93, 1993, pp. 248~259に報告されている。

【0005】これらの方式は効率的であるが、次のような欠点がある。すなわち、これらの方式のうちの最も簡単なものは、悪意のある投票者による選挙妨害を防止しつつ、正当な投票者が選挙の情報遺漏に対して確実に抗議することができないことである。また、選挙後に、各投票者は、彼等の投票が正しく集計されたことをチェックする責任を負うことになる。通常、外部のオブザーバが、選挙が適正に行われたか否かを後に検証する方法はない。さらに、B. Pfitzmannによる文献 "Breaking an efficient anonymous channel" in Eurocrypt' 94 Proceedings, 1994, pp. 339~348に記載されているように、いくつかの匿名チャンネルは、攻撃に対して弱い。

【0006】この発明の教示によれば、外部オブザーバが、選挙が実際に正しく行われたか否かを検証することのできる匿名チャンネルおよび投票方式が提供される。したがって、悪意のある投票者による選挙妨害のおそれなしに、投票の情報遺漏を誰でも検出することができる。さらに、この発明は、また、B. Pfitzmannによって提案された攻撃を妨げるのに役立つ。

【0007】

【発明の概要】同一デスティネーションへの多数のメッセージが、多数のミキシング・センタを経て秘密に伝送

6

される匿名チャンネルが開示されている。送られるメッセージが投票であり、デスティネーションが投票集計センタであり、第1のミキシング・センタが有効投票者のメッセージを受取るならば、この方式は秘密投票方式となる。この発明は、一般に、無記名電子投票がより一般的な発明の実効的な応用である匿名メッセージの伝送方式に関するものである。

【0008】この方式では、センダからの暗号化メッセージは、ミキシング・センタによって逐次的に処理される。最終的にはミキシング・センタがランダムで追跡できない順序で暗号化されていないメッセージの組を出力する。すなわち、匿名チャンネルに用いられた暗号は、各センタで解かれ、最終的には復号される。上位レベルでは、センダはまず自分の暗号化メッセージを公開し、ミキシング・センタ $i$ は、ミキシング・センタ $i-1$  ( $i=1$ の場合にはセンダ) によって公開される各メッセージを処理し、結果を変換し、シャッフルした順序で公開する。

【0009】3つのステップの処理が、各ミキシング・センタ $i$ によって行われる。第1のステップは、各入力メッセージの復号結果を公開する。第2のステップは、各復号結果を変換し、シャッフルした順序で公開する。第3のステップは、ミキシング・センタが第1および第2のステップを正しく実行したことを証明する。文献 "How to Prove Yourself: Practical Solutions to identification and signature problems" in Advances in Cryptology-Crypto' 86, Springer-Verlag, 1986, pp. 186~199に論じられているFiat-Shamir法を用いて、上記ブルーフを相互作用のないようにすることができる。

【0010】3つのステップの処理が終わった後に、利害関係者は、結果のブルーフをチェックして、メッセージが正しく取り扱われたことを確かめる。一般的な検証可能性を実現する方法に対しては、メッセージに冗長性を付加する必要はない。

【0011】また、この発明は、多数のブルーフを1つのブルーフに組合せることによって、ブルーフを生成し、伝送し、チェックするのに必要な通信および演算の量を軽減する方法を与える。

【0012】この発明は、図面を参照した以下の説明により理解できるであろう。

【0013】

【発明の実施の形態】この発明の匿名メッセージ伝送方式を、図1および図2を参照して説明する。この方式によれば、センダ (sender) 10 (1), 10 (2), 10 (3) ... 10 (1) からの暗号化メッセージは、ミキシング・センタ 11 (1), 11 (2), 1

1 (3) ... 11 (n) によって逐次的に処理される。これは、最後のミキシング・センタが、ランダムで追跡できない順序で、復号化されたメッセージの組を出力するまで行われる。演算手段、好適にはパーソナル・コンピュータ（ワークステーション等とすることができる）を備えるセンタによって、投票者は投票する。同様に、各ミキシング・センタは、演算手段、好適にはパーソナル・コンピュータ、ワークステーション等を備えている。センタは、最初に、電子掲示板または他の公開的に利用できるメッセージ手段に、彼等の暗号化メッセージを通知する。ミキシング・センタ11 (i) は、前のミキシング・センタ11 (i-1) (i=1の場合には、センタ10) によって通知された各メッセージを処理して、その結果をシャッフルした順序で公開する。これは、最終のミキシング・センタ11 (n) が、投票の集計結果を公開するまで行われる。この方式の概要を説明したが、どのようにしてメッセージmがセンタによって最初に暗号化されるか、およびどのようにしてミキシング・センタ11 (i) が各メッセージを処理するのかを、以下に詳細に説明する。

【0014】最初に、投票に関するエンティティ、すなわちセンタおよびミキシング・センタは、ある整数kに対して、次の関係が成り立つ

【0015】

$$(G_1, M_1) = (g^{r_0} \bmod p, (w_0)^{r_0} \cdot m \bmod p)$$

を、ミキシング・センタ11 (1) による使用のために公開する。

【0019】説明を簡単にするために、ミキシング・センタの復号、シャッフル、証明の3つのステップを、この順序で説明する。しかし、実行は、このステップを必ずしもこの順序で行わなくてもよい。

【0020】入力  $(G_i, M_i)$  に応じて、ミキシング・センタ11 (i) (i=1, ..., n-1) は、ランダム数  $r_i$  を生成し（各メッセージ対に対し独立に）、秘密鍵  $x_i$  を用いて、次の値、

【0021】

【数5】

\* 【数1】

$$p = kq + 1$$

素数 p, q を用いることに同意する必要がある。値  $g'$  を、 $\bmod p$  の生成元とし、g を、

【0016】

【数2】

$$g = (g')^k \bmod p$$

とする。n 個のミキシング・センタがあると仮定する。

10 各ミキシング・センタ11 (i) は、

【0017】

【数3】

整数  $x_i \in Z_q^*$  を生成し、その公開鍵として、

$$y_i = g^{x_i} \bmod p$$

を公開し、その秘密鍵として  $x_i$  を保持する。簡単にする

20 ために、 $w_i$  は積  $y_{i+1} y_{i+2} \dots y_n$  を示し、 $w_n = 1$  とする。センタ10からのメッセージは、mである。

センタはランダム数  $r_0$  を生成し、

【0018】

\* 【数4】

$$G_{i+1} = G_i \cdot g^{r_i} \bmod p$$

$$= g^{r_0 + \dots + r_i} \bmod p$$

$$H_{i+1} = G_i^{x_i} \bmod p$$

$$M_{i+1} = M_i \cdot w_i^{r_i} / H_{i+1} \bmod p$$

$$= w_i^{r_0 + \dots + r_i} \cdot m \bmod p$$

40 を計算し、 $(G_i, M_i)$  に対応する  $(H_{i+1})$  を公開する。値  $(G_{i+1}, M_{i+1})$  は他の各 i の処理データ間でシャッフルされたあと、ミキシング・センタ11 (i+1) による使用のために公開される。

【0022】ミキシング・センタ11 (i) は、入力  $(G_i, g, y_i, H_{i+1})$  に対して、prove-DECRYPT アルゴリズムを実行する。アルゴリズム prove-DECRYPT の記述は、以下に示される。

このアルゴリズムの実行は、ミキシング・センタ11 (i) が  $H_{i+1}$  を正しく生成したことを証明する。次

50 に、ミキシング・センタ11 (i) は、prove-S

9

HUFFLEアルゴリズムを実行する。アルゴリズム  $p$   $rove-SHUFFLE$  の記述は、以下に示される。このアルゴリズムの実行は、ミキシング・センタが正しくシャッフルしたことを証明する。

【0023】ミキシング・センタ11 (n) は、

【0024】

【数6】

$$m = M_n / G_n^{x_n} \bmod p$$

を演算することによって、入力 ( $G_n$ ,  $M_n$ ) から、 $m$  10  
を回復される。

【0025】次に、ミキシング・センタ11 (n) は、  
入力 ( $G_n$ ,  $g$ ,  $y_i$ ,  $M_n / m$ ) に対しアルゴリズム  
 $prove-DECRYPT$  を実行する。

【0026】アルゴリズム  $prove-DECRYPT$   
および  $prove-SHUFFLE$  について説明する。  
これらアルゴリズムは、ブルーバ (prover) およ  
びベリファイア (verifier) の動作からなる。  
ベリファイアの出力として、以下に説明するように、ラ  
ンダム・ビーコンまたは適当なハッシュ関数の出力とす  
ることができる。 20

【0027】アルゴリズム  $prove-DECRYPT$   
を説明するために、プロトコルの第1ステップを、以下  
に概説する。最初のステップは、与えられた  $G$  に対して  
復号を実行し、 $H = G^x \bmod p$  を生成する。ブルー  
バは、( $G$ ,  $g$ ,  $y = g^r \bmod p$ ,  $H$ ) が与えられ  
た時に、 $H$  がこのように  $G$  から生成されたことを示して  
いる。アルゴリズムは、次のとおりである。  $prove-$   
 $DECRYPT$

1. ブルーバは、一様に、

【0028】

【数7】

$r \in \mathbb{Z}_{p-1}$  を選択する。

$$y' = g^r \bmod p$$

$$G' = G^r \bmod p$$

ブルーバは、( $y'$ ,  $G'$ ) を送る。

【0029】2 a. 確率  $1/2$  で、ベリファイアは、プ  
ルーバに  $r$  を示すことを要求する。ベリファイアは、  
 $y'$  および  $G'$  が  $r$  と矛盾しないことをチェックする。 40

【0030】2 b. 確率  $1/2$  で、ベリファイアは、プ  
ルーバに  $r' = r - x$  を示すことを要求する。ベリフ  
アイアは、

【0031】

【数8】

10

$$y' = g^{r'} \cdot y \bmod p \text{ and}$$

$$G' = H \cdot G^{r'} \bmod p$$

をチェックする。

アルゴリズムの終了

アルゴリズム  $prove-SHUFFLE$  を説明するた  
めに、プロトコルの第2のステップを、以下に概説す  
る。

【0032】定数  $g$ ,  $w$  および

【0033】

【数9】

$$A = \begin{pmatrix} a_1^{(1)} \\ a_1^{(2)} \end{pmatrix}$$

が与えられた時に、第2のステップは、 $r_1$ ,  $r_2$ , ...  
と置換  $\pi$  を生成し、対の集合

【0034】

【数10】

$$B = \begin{pmatrix} a_{\pi(1)}^{(1)} \cdot g^{r'} \pi(1) \bmod p \\ a_{\pi(1)}^{(2)} \cdot w^{r'} \pi(1) \bmod p \end{pmatrix}$$

を生成することからなる。ここで  $a_1^{(1)}$  は第1ステッ  
プの  $G$  であり、 $a_1^{(2)}$  は  $M/H$  である。ブルーバは、  
( $A$ ,  $B$ ,  $g$ ,  $w$ ) が与えられた時に、 $B$  は  $A$  からこの  
ようにして生成されたことを示している。アルゴリズム  
は、次のとおりである。  $prove-SHUFFLE$

1. ブルーバは、一様に、

【0035】

【数11】

$t \in \mathbb{Z}_{p-1}$ , ランダム置換  $\lambda$  を選び

$$C = \begin{pmatrix} a_{\lambda(1)}^{(1)} \cdot g^t \lambda(1) \bmod p \\ a_{\lambda(1)}^{(2)} \cdot w^t \lambda(1) \bmod p \end{pmatrix}$$

を計算する。

【0036】ブルーバは、 $C$  を送る。

【0037】2 a. 確率  $1/2$  で、ベリファイアは、プ  
ルーバに  $\lambda$  および  $t_i$  を示すことを要求する。ベリフ  
アイアは、 $C$  が  $A$ ,  $\lambda$ ,  $t_i$  と矛盾しないことをチェック  
する。

【0038】2 b. 確率  $1/2$  で、ベリファイアはブル  
ーバに、 $\lambda' = \lambda$ ,  $\pi^{-1}$  および  $t'_i = t_i - r'_i$  を  
示すことを要求する。ベリファイアは、次のようにし

て、 $B$  から  $C$  を生成できることをチェックする。 50

【0039】

【数12】

$$B = \begin{pmatrix} b_1^{(1)} \\ b_1^{(2)} \end{pmatrix}$$

に対し

【0040】

【数13】

$$C = \begin{pmatrix} b_{\lambda'}^{(1)} \cdot g^{t' \lambda' (1)} \bmod p \\ b_{\lambda'}^{(2)} \cdot w^{t' \lambda' (1)} \bmod p \end{pmatrix}$$

が成り立つ。アルゴリズムの終了アルゴリズム  $\text{prove-DECRYPT}$  または  $\text{prove-SHUFFLE}$  の各実行は、確率  $1/2$  で、不正ブルーバを発見する。この確率を1に高めるために、独立の複数回の実行が必要となる。

【0041】上記のアルゴリズムはベリファイアの出方によって記述されているが、より効率的な解決法は、相互作用を排除する Fiat-Shamir 法を用いることである。第1に、プロトコルを多数回（約40または60）実行して、すべてのチャレンジ（challenge）に耐える確率を非常に小さくする。次に、ベリファイアを、擬似乱数を発生する適切なハッシュ関数によって置き換えられる。このハッシュ機能は、アルゴリズム  $\Delta \text{prove-DECRYPT}$  または  $\text{prove-SH}$

$$\prod_i (H^{(j)})^{c_j} = \prod_i ((G^{(j)})^{c_j})^x \bmod p$$

したがって  $G = \prod_i (G^{(j)})^{c_j}$  および  $H = \prod_i (H^{(j)})^{c_j}$  として上記プロトコルを、センタは実行すればよい。1つ以上の元の式が誤っている場合は、係数がランダムに選ばれる限り、最後の式は高い確率で誤る。これらのランダム係数は、ブルーバによって選ばれてはならず、ベリファイア、ビーコンによって、あるいは適切なハッシュ機能の出力として、与えられなければならない。

【0046】同様に、上記方式の変形として、以下の2ラウンド（round）匿名チャンネルを、構成することができる。2ラウンド匿名チャンネルにおいて、各ミキシング・センタ11(i)は、入力  $(G_i, M_i)$  があると、まず最初に、入力を  $(G_i \cdot g^{r_i} \bmod p, M_i \cdot w^{r_i} \bmod p)$  とシャッフルし、シャッフルされた値をランダムな順序で次のセンタに通過させる。各センタは、 $\text{prove-SHUFFLE}$  アルゴリズムを実行して（この方式に対して一定のいくつかの定数で）、情報の正しさを証明する。シャッフルされた

\*UFFLEのステップ1におけるブルーバの公開メッセージから、チャレンジを生成する。Fiat-Shamir法のこの発見的手法は、文献“*How to Prove Yourself: Practical solutions to identification and signature problems*” in *Advances in Cryptology-Crypto' 86*, Springer-Verlag, 1986, pp. 186~199に記載されている。このようにすれば、ブルーバは、すべてのメッセージを1つの電文にしてベリファイアに送ることができる。このメッセージは、公開アクセスに対し公開される。

【0042】前のセンタからの各メッセージについてアルゴリズム  $\text{prove-DECRYPT}$  を実行するのに要求される演算および通信の量を、軽減することができる。複数のブルーバを1つのブルーバに統合することによって、センタは、彼等がすべての入力を正確に復号したことを効率的に証明することができる。

20 【0043】次式が各対  $(G^{(j)}, H^{(j)})$  について成文を示すことを示す必要がある。

【0044】

【数14】

$$H^{(j)} = (G^{(j)})^x \bmod p$$

上式は、ランダムに選ばれた係数  $c_i$  を用いることによって、次の1つの式に置き換えることができる。

【0045】

【数15】

メッセージは、最後にミキシング・センタ11(n)に与えられ、各メッセージに対し  $G_{n+1}$  および  $M_{n+1}$  を公開する。次に、各ミキシング・センタ11(i)は  $H_i = G_{n+1}^{c_i}$  を公開する。ミキシング・センタ11(i)は、入力  $(G_{n+1}, g, H_i)$  に対し  $\text{prove-DECRYPT}$  アルゴリズムを実行し、正しさを証明する。メッセージ  $m$  は、 $M_{n+1} / \prod H_i$  によって復号することができる。

40 【0047】模倣投票の攻撃を避けるために、各センタは、通知すべきメッセージを署名することによって暗号化することができる。メッセージ・コンストラクタ（以下に説明する）の出力を署名し、第1センタ11(1)の公開鍵を用いてメッセージを暗号化することによって、悪意の投票者は、他のセンタのメッセージをコピーすることはできない。というのは、コピーされたメッセージは、正しい署名を有さないからである。さらに、メッセージは暗号化されているので、異なる署名が暗号化メッセージに付くようにも操作できない。



13

【0048】あるいはまた、第1のセンタは、各センタがノートあるいはメッセージを通知するまで、センタからのすべてのメッセージを秘密にすることができる。

【0049】第1のセンタ11(1)および悪意のセンタが共謀することを防止するためには、M. Naorによる文献“Bit commitment using pseudo-randomness,” in Advances in Cryptology-CRYPTO' 89, 1989, pp. 128~136に論じられているような普通の秘密コミットメント方式を用いることが可能である。

【0050】この発明を実施する好適な方法を説明したが、次に、この発明を実施するのに有用な好適な実施例を説明する。

【0051】図1は、この発明を実施する好適な実施例を示す。センダ10(1)、10(2)、10(3)…10(n)およびミキシング・センタ11(1)、11(2)、11(3)…11(n)は、普通の電子掲示板12に接続されたパーソナル・コンピュータまたはワークステーションを使用する。メッセージ伝送プロセスに対するすべての当事者(センダ、ベリファイア、センタ等)は、掲示板にメッセージを通知し、および掲示板からのメッセージを受信することによって、相互に作用する。センダは、センタとして機能することもできる。パーソナル・コンピュータは、上述した方法を実施するソフトウェアを含むか、あるいは図2に示す要素のハードウェアまたはソフトウェアの実施を含む。

【0052】図2は、どのようにメッセージが匿名で伝送されるかを示している。メッセージ・センダ10(1)、10(2)、10(3)…10(n)の各メッセージ・コンストラクタ14(1)、14(2)、14(3)…14(n)は、上述した定数15を用いて、暗号化されたメッセージ16(1)、16(2)、16(3)…16(n)を生成する。暗号化メッセージは、電子掲示板12に公開される。次に、各ミキシング・センタ11(i)は、掲示板12からのメッセージ17(i-1)を、その入力として読取る。(ミキシング・センタ11(1)は、暗号化メッセージ16を読取る)次に、ミキシング・センタは、前述したように、その秘密鍵23(i)を用いて、連続してプロセス復号19、シャッフル20、prove-DECRYPT21、prove-SHUFFLE22を実行する。処理されたメッセージおよびブルーフ17(i)は、電子掲示板に公開される。(ミキシング・センタ11(n)は、復号されたメッセージ18を公開する。)電子投票の場合、ミキシング・センタ11(n)は、投票の結果を公開する。

【0053】図3は、チャンネル・チェッカ24を模式的に示す。チャンネル・チェッカ24は、定数15、暗号化メッセージ16、1組の処理されたメッセージおよびブルーフ17(i)、17(2)、…、復号メッセージ18を受信し、メッセージ伝送が上述したように処理されたかどうかを決定し、チャンネルとして有効あるいは無効であったかを判定する。すなわち、チャンネル・チェッカは、ミキシング・センタによって与えられるブルーパのためのベリファイアを含んでいる。

【0054】図4はメッセージ・コンストラクタ14を示す。メッセージ・コンストラクタ14は、前述した定数15を用いて、メッセージ25に対し暗号化メッセージ16を生成する。

【0055】匿名メッセージ伝送および電子投票の好適な方法および装置について説明したが、当業者には、この発明の広い教示と趣旨から逸脱することなく、変形、変更が可能である。

#### 【図面の簡単な説明】

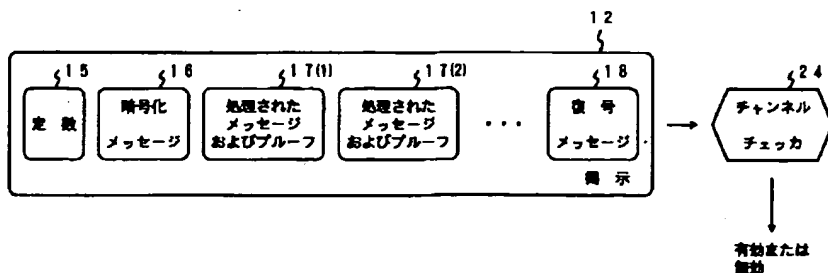
【図1】この発明を実施する好適な実施例の模式図である。

【図2】メッセージ・フローの模式図である。

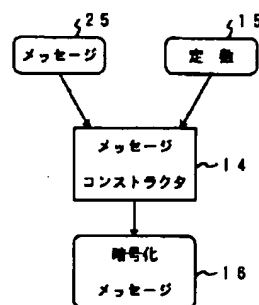
【図3】チャンネル・チェッカの模式図である。

【図4】メッセージ・コンストラクタの模式図である。

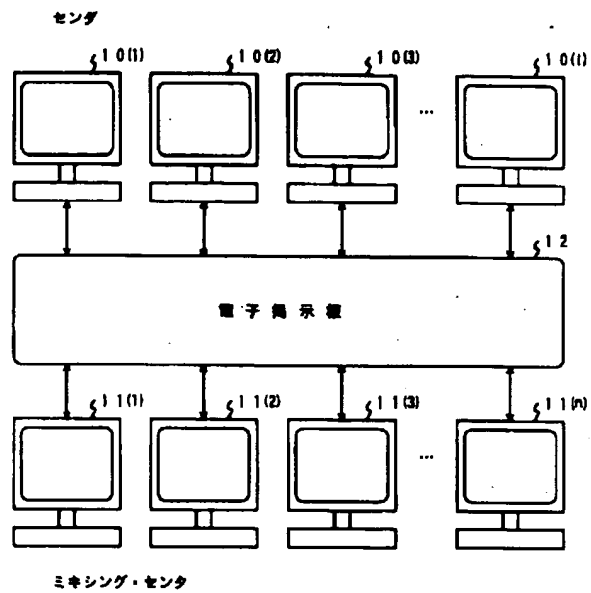
【図3】



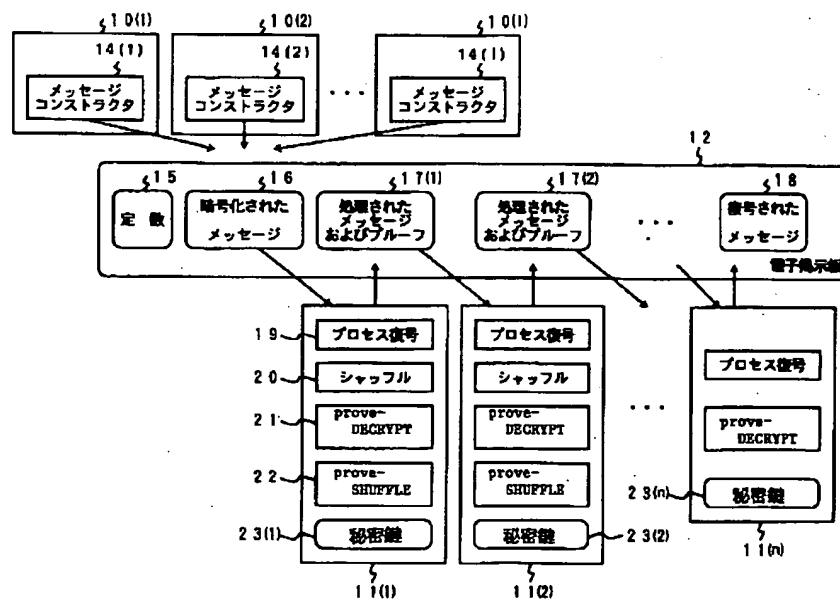
【図4】



【図1】



【図2】



【外国語明細書】

## 1. Title of Invention

### Secure Anonymous Message Transfer and Voting Scheme

## 2. Claims

1. A method of secure anonymous message transfer from a plurality of senders by use of a plurality of mixing centers comprising the steps of:
  - (a) choosing constants which are posted for senders  $S_1, S_2, \dots, S_l$  and mixing centers,  $C_1, C_2, \dots, C_n$ ;
  - (b) each sender  $S_k$  constructing an encrypted message which is posted;
  - (c) a first mixing center  $C_1$  processing the posted messages from each sender  $S_k$  which processed messages are then posted for use by the next center;
  - (d) each mixing center  $C_2$  through  $C_{n-1}$  sequentially processing the processed messages from the previous center,, which sequentially processed messages are then posted for use by the next center;
  - (e) the last mixing center  $C_n$  processing messages from the previous center  $C_{n-1}$  and posting the result;
  - (f) each mixing center proving the validity of its processing, which proof is posted; and
  - (g) channel checker verifying correctness of the execution from posted messages when necessary.

2. A method of secure anonymous message transfer as set forth in claim 1, where steps (c),(d) and (e) further comprises:
  - (h) providing each mixing center with a secret key; and
  - (i) said processing including using the secret key of a respective mixing center.
3. A method of secure anonymous message transfer as set forth in claim 2, where said proving comprises executing algorithm prove-DECRYPT.
4. A method of secure anonymous message transfer as set forth in claim 3, where said executing algorithm prove-DECRYPT is executed for multiple messages together.
5. A method of secure anonymous message transfer as set forth in claim 2, where said proving comprises applying the Fiat-Shamir method.
6. A method of secure anonymous message transfer as set forth in claim 2, further comprising (j) shuffling the messages.
7. A method of secure anonymous message transfer as set forth in claim 6, where said proving further comprises executing algorithm prove-SHUFFLE.

8. A method of secure anonymous message transfer as set forth in claim 1, where steps (c), (d), and (e) further comprises shuffling the messages.
9. A method of secure anonymous message transfer as set forth in claim 8, where after the last mixing center  $C_n$  posts the result, each mixing center executes algorithm `prove-DECRYPT` using the result.
10. A method of secure anonymous message transfer as set forth in claim 8, further comprising providing each mixing center with a secret key and where after the last mixing center  $C_n$  posts the result, each mixing center performs said processing using its respective secret key and the result.
11. A method of secure anonymous message transfer as set forth in claim 8, where said proving comprises executing algorithm `prove-SHUFFLE`.
12. A method of secure anonymous message transfer as set forth in claim 11, where said proving comprises applying the Fiat-Shamir method.
13. A method of secure anonymous message transfer as set forth in claim 8, where said proving comprises applying the Fiat-Shamir method.
14. A method of secure anonymous message transfer as set forth in claim 1, where said proving comprises applying the Fiat-Shamir method.

15. A method of secure anonymous message transfer as set forth in claim 1, where in step (b) each sender  $S_k$  posts its encrypted message substantially simultaneously.
16. A method of secure anonymous message transfer as set forth in claim 1, where in step (b) each sender  $S_k$  constructs its encrypted message using a key of said first mixing center  $C_1$  and said encrypted message includes a signature of a respective sender  $S_k$ .
17. A method of secure anonymous message transfer as set forth in claim 1, where in step (b) each sender  $S_k$  constructs an encrypted message which is publicly revealed after said first mixing center  $C_1$  receives a respective encrypted message.
18. A method of secure anonymous message transfer as set forth in claim 1, said first mixing center  $C_1$  processing only legitimate messages and processing only one message from each sender.
19. A method of secure anonymous message transfer as set forth in claim 18, where said senders are voters and said messages are votes.
20. A method of secure anonymous message transfer as set forth in claim 19, where said processing of said last mixing center  $C_n$  comprises computing a tally.

21. An apparatus for secure anonymous message transfer comprising:

a bulletin board having constants;

a plurality of senders,  $S_1, S_2, \dots, S_t$ , each sender  $S_k$  constructing an encrypted message using the constants and posting said encrypted message to said bulletin board;

a plurality of mixing centers,  $C_1, C_2, \dots, C_n$ , a first mixing center  $C_1$  processing the posted messages from each sender using the constants and posting a processed message to said bulletin board for use by the next mixing center, each mixing center  $C_2$  through  $C_{n-1}$  sequentially processing the processed message from the previous mixing center using the constants and posting a further processed message to said bulletin board for use by the next mixing center, the last mixing center  $C_n$  processing messages from the previous center  $C_{n-1}$  using the constants and posting the result on said bulletin board;

means associated with each respective mixing center for proving the validity of the processing of the respective mixing center, which proof is posted on said bulletin board; and

channel checking means for verifying the correctness of execution from posted messages.

22. An apparatus for anonymous message transfer as set forth in claim 21, further comprising secret key means associated with each respective mixing center for providing a secret key to said respective mixing center for processing messages.

23. An apparatus for anonymous message transfer as set forth in claim 22, where said mixing center processes messages by executing algorithm prove-DECRYPT.
24. An apparatus for anonymous message transfer as set forth in claim 23, where each said means associated with each respective mixing center executes algorithm prove-DECRYPT.
25. An apparatus for anonymous message transfer as set forth in claim 24, where each means associated with each respective mixing center executes algorithm prove-DECRYPT for multiple messages.
26. An apparatus for anonymous message transfer as set forth in claim 21, where said mixing center processes messages by shuffling messages.
27. An apparatus for anonymous message transfer as set forth in claim 26, where said mixing centers process messages by executing algorithm prove-SHUFFLE.
28. An apparatus for anonymous message transfer as set forth in claim 26, where each said means associated with each respective mixing center executes algorithm prove-SHUFFLE.



29. An apparatus for anonymous message transfer as set forth in claim 21, where each sender  $S_k$  posts its encrypted message to said bulletin board substantially simultaneously.
30. An apparatus for anonymous message transfer as set forth in claim 22, where each sender  $S_k$  constructs its encrypted message using said secret key of said first mixing center  $C_1$  and including a signature of the respective sender  $S_k$ .
31. An apparatus for anonymous message transfer as set forth in claim 21, where each sender constructs an encrypted message which is publicly revealed after said first mixing center  $C_1$  receives a respective encrypted message.
32. An apparatus for anonymous message transfer as set forth in claim 21, said first mixing center  $C_1$  processing only legitimate messages and processing only one message from each sender.
33. An apparatus for anonymous message transfer as set forth in claim 32, where said senders are voters and said messages are votes.
34. An apparatus for anonymous message transfer as set forth in claim 33, where said result comprises a tally.

### 3. Detailed Description of Invention

#### Field of Invention

The present invention relates to secure anonymous message transfer and specifically, to number-theoretic methods and apparatus for secure electronic voting.

#### Background of the Invention

Secure electronic voting is one of the most important applications of secure multi-party computation. Yet despite extensive work on this subject, no complete solution has been found in either the theoretical or practical domains. Even the general solutions to secure multi-party protocols fail to exhibit all of the desired security properties of elections.

A number of more practical voting protocols have been proposed, with widely differing security properties. Schemes based on anonymous channels/mixers have become very popular due to their superior efficiency and the arbitrary nature of the votes that are allowed.

Mix-net anonymous channels were first proposed by D. Chaum in an article entitled "Untraceable Electronic Mail, Return Address, and Digital Pseudonyms" in *Communication of the ACM*, ACM, 1981, pp 84 to 88. Subsequently, many voting schemes have been proposed based on this basic technique as in an article by A. Fujioka et al, entitled "A Practical Secret Voting Scheme for Large Scale Elections," in *Advances in Cryptology - Auscrypt '92*, 1992, pp. 244 to 251, and in an article by C. Park et al, entitled "All/Nothing Election Scheme and Anonymous Channel" in *Advances in Cryptology, Eurocrypt '93*, 1993, pp. 248 to 259.

These schemes are efficient, but have the following shortcomings. The simplest of these schemes does not allow a voter to securely protest the omission of a vote without allowing a malicious voter to block the election. After the election, each

voter is typically responsible for checking that their vote was correctly tallied. There is usually no way for an outside observer to later verify that the election was properly performed. Furthermore, some anonymous channels are vulnerable to an attack as described in an article by B. Pfitzmann entitled "Breaking an efficient anonymous channel" in Eurocrypt '94 Proceedings, 1994, pp. 339 to 348.

In accordance with the teachings of the present invention, a secure anonymous channel and a voting scheme are described in which an outside observer can verify that the election was indeed performed correctly. Therefore omission of a vote can be detected by anyone, without fear of a malicious voter blocking the election. Furthermore, the present invention also helps thwart an attack proposed by B. Pfitzmann, *supra*.

#### Summary of the Invention

A secure anonymous channel is described where multiple messages to a same destination are transferred securely through multiple mixing centers. If the messages to be sent are votes where the destination is a vote-counting center and the first mixing center accepts messages of valid voters, then this scheme becomes a secure voting scheme. The present invention generally refers to an anonymous message transfer scheme where secure electronic voting is a practical application of the more general invention.

In the scheme, encrypted messages from the senders are successively processed by the mixing centers until the last center outputs a randomly, untraceably ordered set of unencrypted messages. That is, the encryptions used for the anonymous channel have been stripped off or decrypted. At a high level, the senders first post their encrypted messages. mixing center  $i$  processes each message posted by mixing center  $i - 1$  (or the senders, when  $i = 1$ ) and posts the results in permuted order.

A three-step procedure is followed by each mixing center  $i$ . The first step is posting decrypted results of each input message. The second step is mixing the results and posting them in permuted order. The third step is proving that the centers correctly executed the first and second steps. The Fiat-Shamir technique as discussed in an article entitled "How to Prove Yourself: Practical Solutions to identification and signature problems" in *Advances in Cryptology - Crypto '86*, Springer-Verlag, 1986, pp. 186 to 199, can be used to make the above proofs non-interactive.

At the conclusion of the three step process or at a later time, any interested party can check the resulting proofs to confirm that the messages have all been handled correctly. With this method for achieving universal verifiability there is no need for adding redundancy to the messages.

Also, the invention results in a method which reduces the amount of communication and computation necessary to generate, transmit and check the proofs by combining multiple proofs into a single proof.

The present invention will be best understood when the following description is read in conjunction with the accompanying drawing.

#### Detailed Description of the Invention

The anonymous message transfer scheme comprising the present invention will now be described with reference to Figures 1 and 2. In accordance with the scheme, encrypted messages from senders  $10(1)$ ,  $10(2)$ ,  $10(3)$ ... $10(l)$  are successively processed by the mixing centers  $11(1)$ ,  $11(2)$ ,  $11(3)$ ... $11(n)$  until the last center provides as its output a randomly, untraceably ordered set of unencrypted messages. Voters cast their ballot by means of a sender which comprises a computing means, preferably a personal computer but it may also be a workstation or the like. Similarly, each mixing center comprises a computing means, preferably a personal computer, a workstation or the like. The senders first post their encrypted messages preferably on an electronic bulletin board or other publicly

available messaging means. Mixing center 11(*i*) processes each message posted by the previous mixing center 11(*i* - 1) (or the senders 10, when *i* = 1) and posts the results in permuted order until the last mixing center 11(*n*) posts the result or tally of the voting. Having set forth an overview of the scheme, the detail of how a message *m* is initially encrypted by a sender and how a mixing center 11(*i*) processes each message will now be described in detail.

Initially, entities participating in the voting, i.e. the senders and the mixing centers, need to agree on using prime numbers *p* and *q* where the following relationships exist for some integer *k*:

$$p = kq + 1.$$

The value *g'* is a generator mod *p* and *g* is equal to

$$g = (g')^k \text{ mod } p.$$

Assume there are *n* mixing centers. Each mixing center 11(*i*) generates a integer  $x_i \in Z_q^*$  and publishes

$$y_i = g^{x_i} \text{ mod } p$$

as its public key and keeps *x<sub>i</sub>* as its secret key. For the purpose of simplification, *w<sub>i</sub>* will represent the product  $y_{i+1}y_{i+2} \cdots y_n$  and  $w_n = 1$ .

The message from a sender 10 is *m*. The sender generates a random number *r<sub>0</sub>*, and posts

$$(G_1, M_1) = (g^{r_0} \text{ mod } p, (w_0)^{r_0} \cdot m \text{ mod } p)$$

for use by mixing center 11(1).

For ease of explanation, the three steps of decrypt, shuffle and prove of the centers will be described in this order. However, implementation does not necessarily require the steps to be performed in this order.

In response to input  $(G_i, M_i)$ , mixing center 11  $i$  ( $i = 1, \dots, n-1$ ) generates a random number  $r_i$  (independently for each message-pair) and calculates the following values using the secret key  $x_i$ :

$$\begin{aligned} G_{i+1} &= G_1 \cdot g^{r_1} \bmod p \\ &= g^{r_0 + \dots + r_1} \bmod p \\ H_{i+1} &= G_1^{x_1} \bmod p \\ M_{i+1} &= M_1 \cdot w_1^{r_1} / H_{i+1} \bmod p \\ &= w_1^{r_0 + \dots + r_1} \cdot m \bmod p \end{aligned}$$

and posts  $(H_{i+1})$  corresponding to  $(G_i, M_i)$ . The value  $(G_{i+1}, M_{i+1})$  is posted, permuted with the other processed messages for use by mixing center 11  $(i+1)$ .

The mixing center 11( $i$ ) executes a prove-DECRYPT algorithm for inputs  $(G_i, g, y_i, H_{i+1})$ . The description of the algorithm prove-DECRYPT is given in below. Execution of this algorithm proves that mixing center 11( $i$ ) generated  $H_{i+1}$  correctly. Mixing center 11( $i$ ) then executes a prove-SHUFFLE algorithm, a description of which is given below. Execution of this algorithm proves that the mixing center shuffled honestly.

Mixing center 11( $n$ ) recovers  $m$  from input  $(G_i, M_i)$  by computing:

$$m = M_n / G_n^{x_n} \bmod p.$$

The mixing center 11( $n$ ) then executes the prove-DECRYPT algorithm for inputs  $(G_n, g, y_i, M_n/m)$ .

The algorithms prove-DECRYPT and prove-SHUFFLE will now be described. The algorithms involve a prover and a verifier. The verifier may be a random beacon or an output of a suitable hash function, as is described below.

In order to describe the algorithm prove-DECRYPT, the first phase of the protocol is abstracted as follows. Given  $G$ , the first step comprises performing decryption in order to generate  $H = G^x \bmod p$ . The proof comprises, given  $(G, g, y = g^x \bmod p, H)$ , showing that  $H$  is generated in this manner from  $G$ . The algorithm is as follows:

#### prove-DECRYPT

1. The prover uniformly chooses  $r \in Z_{p-1}$ .

$$\text{Let } y' = g^r \bmod p$$

$$G' = G^r \bmod p.$$

The prover sends  $(y', G')$ .

- 2a. With probability  $\frac{1}{2}$ , the verifier asks the prover to reveal  $r$ . The verifier checks that  $y'$  and  $G'$  are consistent with  $r$ .
- 2b. With probability  $\frac{1}{2}$ , the verifier asks the prover to reveal  $r' = r - x$ . The verifier checks that

$$y' = g^{r'} \cdot y \bmod p \text{ and}$$

$$G' = H \cdot G^{r'} \bmod p.$$

end of algorithm

In order to describe the algorithm prove-SHUFFLE, the second step is abstracted as follows.

Given constants  $g, w$  and

$$A = \begin{pmatrix} a_i^{(1)} \\ a_i^{(2)} \end{pmatrix},$$

the second step comprises generating  $r_1, r_2, \dots$  and a permutation  $\pi$  and generating a set of pairs

$$B = \begin{pmatrix} a_{\pi(i)}^{(1)} \cdot g^{r'_{\pi(i)}} \bmod p \\ a_{\pi(i)}^{(2)} \cdot w^{r'_{\pi(i)}} \bmod p \end{pmatrix}.$$

Here  $a_i^{(1)}$  refers to  $G$ 's and  $a_i^{(2)}$  refers to  $M/H$ 's in the first step. The proof comprises, given  $(A, B, g, w)$ , showing that  $B$  could be generated in this manner from  $A$ . The algorithm is as follows:

#### prove-SHUFFLE

1. The prover uniformly chooses  $t \in Z_{p-1}$ , random permutation  $\lambda$  and

$$C = \begin{pmatrix} a_{\lambda(i)}^{(1)} \cdot g^{t_{\lambda(i)}} \bmod p \\ a_{\lambda(i)}^{(2)} \cdot w^{t_{\lambda(i)}} \bmod p \end{pmatrix}.$$

The prover sends  $C$ .

- 2a. With probability  $\frac{1}{2}$ , the verifier asks the prover to reveal  $\lambda$  and  $t_i$ . The verifier checks that  $C$  is consistent with  $A, \lambda, t_i$  in that way.



- 2b. With probability  $\frac{1}{2}$ , the verifier asks the prover to reveal  $\lambda' = \lambda \circ \pi^{-1}$  and  $t'_i = t_i - r'_i$ . The verifier checks that  $C$  can be generated from  $B$  in the following way:

$$\text{For } B = \begin{pmatrix} b_1^{(1)} \\ b_1^{(2)} \end{pmatrix},$$

$$C = \begin{pmatrix} b_{\lambda' (1)}^{(1)} \cdot g^{t' \lambda' (1) \bmod p} \\ b_{\lambda' (1)}^{(2)} \cdot w^{t' \lambda' (1) \bmod p} \end{pmatrix} \text{ holds.}$$

End of algorithm

Each execution of the algorithms `prove-DECRYPT` or `prove-SHUFFLE` finds a cheating prover with probability  $\frac{1}{2}$ . In order to raise this probability closer to 1, independent executions are necessary.

While these algorithms are given in terms of a verifier, a more efficient solution is to use the Fiat-Shamir method of eliminating interaction. First, the protocol is run many times (on the order of 40 or 60) in order to make the probability of withstanding all of the challenges exceedingly small. Then the verifier is replaced by a suitably "random looking" hash function which generates the challenges from the prover's posting in Step 1 of the algorithms `prove-DECRYPT` or `prove-SHUFFLE`. This heuristic of Fiat-Shamir method is described in an article entitled "How to Prove Yourself: Practical solutions to identification and signature problems" in *Advances in Cryptology- Crypto '86*, Springer-Verlag, 1986, pp. 186 to 199. This way the prover can send all the messages to the verifier in a single message. This message is posted for public access.

The bulk of the computation and communication required to execute algorithm **prove-DECRYPT** for each of the messages from previous centers can be reduced. By combining many of the proofs into a single proof, the centers can efficiently prove they decrypted all of the inputs correctly.

It is necessary to show that the following equation holds for each pair  $(G^{(j)}, H^{(j)})$ .

$$H^{(j)} = (G^{(j)})^x \bmod p$$

The above equations are reduced to the following single equation using randomly chosen coefficients  $c_j$ :

$$\prod_i (H^{(j)})^{c_j} = \prod_i ((G^{(j)})^{c_j})^x \bmod p$$

A center can execute the above protocol where

$$G = \prod_i (G^{(j)})^{c_j} \text{ and } H = \prod_i (H^{(j)})^{c_j}.$$

Advantage is made of the fact that if one or more of the original equations is wrong, then if the coefficients are chosen randomly, the final equation will also be wrong with high probability. These random coefficients must not be chosen by the prover, but should be provided by a verifier, beacon or as the output of a suitable hash function.

Similarly, as a variation of the above scheme, the following two round anonymous channel can be constructed. In the two round anonymous channel, each mixing center 11(i), on inputs  $(G_i, M_i)$  first shuffles the inputs to  $(G_i \cdot g^{r_i} \bmod p, M_i \cdot w_0^{r_i} \bmod p)$  and passes the shuffled values in a random order to the next center. Each center executes the prove-SHUFFLE algorithm (with some constants fixed to this scheme) to prove the correctness of the information. When the shuffled messages are finally provided to the mixing center 11(n), mixing center 11(n) publishes  $G_{n+1}$  and  $M_{n+1}$  for each message. Then each mixing center 11(i) publishes  $H_i = G_{n+1}^{x_i}$ . The mixing center 11(i) executes the prove-DECRYPT algorithm with input  $(G_{n+1}, g, H_i)$  to prove the correctness. The message  $m$  can be recovered by  $M_{n+1} / \prod H_i$ .

In order to avoid vote-duplication attack, each sender may sign and encrypt the message to be posted. That is, the sender may sign the output of a message constructor (described below) and then encrypting the message using the public key of the first center 11(1), a malicious sender cannot copy another sender's message, since the copied message would not have the correct signature. Moreover, the message is encrypted in a manner such that the message cannot be decrypted, nor can a different signature be affixed to the encrypted message.

Alternatively, the first center may conceal all of the message from the senders until each sender has posted a note or message.

In order to prevent the first center 11(1) and a malicious sender from conspiring, it is possible to use a conventional secure commitment scheme such as that discussed in an article by M. Naor, entitled "Bit commitment using pseudo-randomness," in *Advances in Cryptology - CRYPTO '89*, 1989, pp. 128 to 136.

Having described a preferred method of practicing the present invention, preferred embodiments useful for practicing the invention will now be described.

Figure 1 schematically illustrates a preferred embodiment for practicing the invention. The senders  $10(1)$ ,  $10(2)$ ,  $10(3)$ ,...  $10(\ell)$  and mixing centers  $11(1)$ ,  $11(2)$ ,  $11(3)$ ... $11(n)$  use personal computers or workstations connected to a conventional electronic bulletin board 12. All parties (senders, verifiers, centers and the like) to the message transfer process interact by posting messages to and receiving messages from the bulletin board. Senders can also serve as centers. The personal computers either contain software to perform the method described above or alternatively contain in hardware or software embodiments of the elements described in Figure 2.

Figure 2 illustrates how messages are anonymously transferred. Each message constructor  $14(1)$ ,  $14(2)$ ,  $14(3)$ ... $14(\ell)$  of message sender  $10(1)$ ,  $10(2)$ ,  $10(3)$ ... $10(\ell)$  generates an encrypted message  $16(1)$ ,  $16(2)$ ,  $16(3)$ ,... $16(\ell)$ , using constants 15 as described above. The encrypted messages 16 are posted to the electronic bulletin board 12. Then each mixing center  $11(i)$  reads as its input, message  $17(i-1)$  from the bulletin board 12. (mixing center  $11(1)$  reads the encrypted message 16.) The mixing center then follows the sequence process decrypt 19, shuffle 20, prove-DECRYPT 21, prove-SHUFFLE 22 using its secret key  $23(i)$  as described above. The processed messages and proofs  $17(i)$  are posted to the electronic bulletin board. (Mixing center  $11(n)$  posts decrypted messages 18.) In the case of electronic voting, mixing center  $11(n)$  will post a tally of the votes

Figure 3 schematically illustrates a channel checker 24. The channel checker 24 receives constants 15, encrypted messages 16, a set of processed messages and proofs  $17(1)$ ,  $17(2)$ ... and decrypted messages 18 and determines whether the message transfer was processed as specified above, thus indicating a valid or invalid channel. That is, the channel checker includes a verifier for the proofs given by the mixing centers.

Figure 4 illustrates a message constructor 14. The message constructor 14 generates encrypted message 16 for the message 25 using constants 15 as described above.

While there has been described and illustrated a preferred method and apparatus of secure anonymous message transfer and electronic voting, it will be apparent to those skilled in the art that variations and modifications are possible without deviating from the broad teachings and spirit of the present invention which shall be limited solely by the scope of the claims appended hereto.

#### **4. Brief Description of Drawings**

**Figure 1** is a schematic illustration of a preferred embodiment for practicing the present invention;

**Figure 2** is a schematic illustration of message flow;

**Figure 3** is a schematic illustration of a channel checker; and

**Figure 4** is a schematic illustration of a message constructor.

Fig. 1

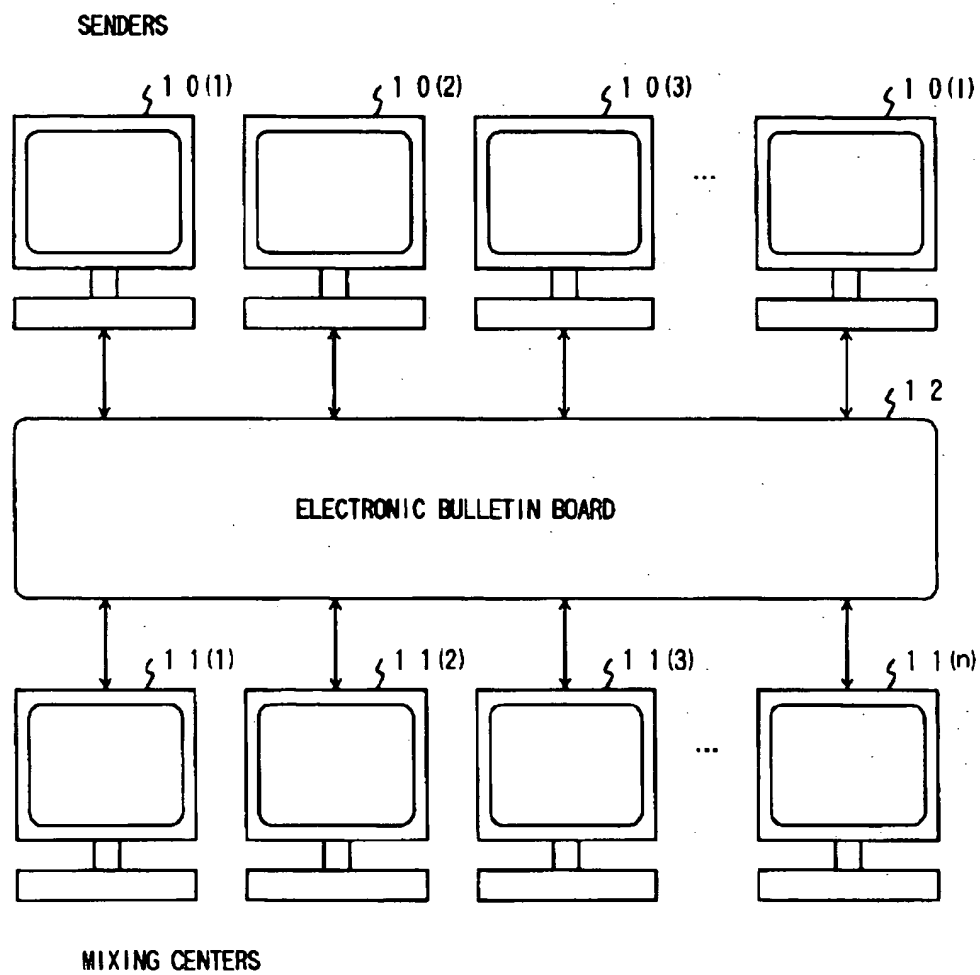


Fig.2

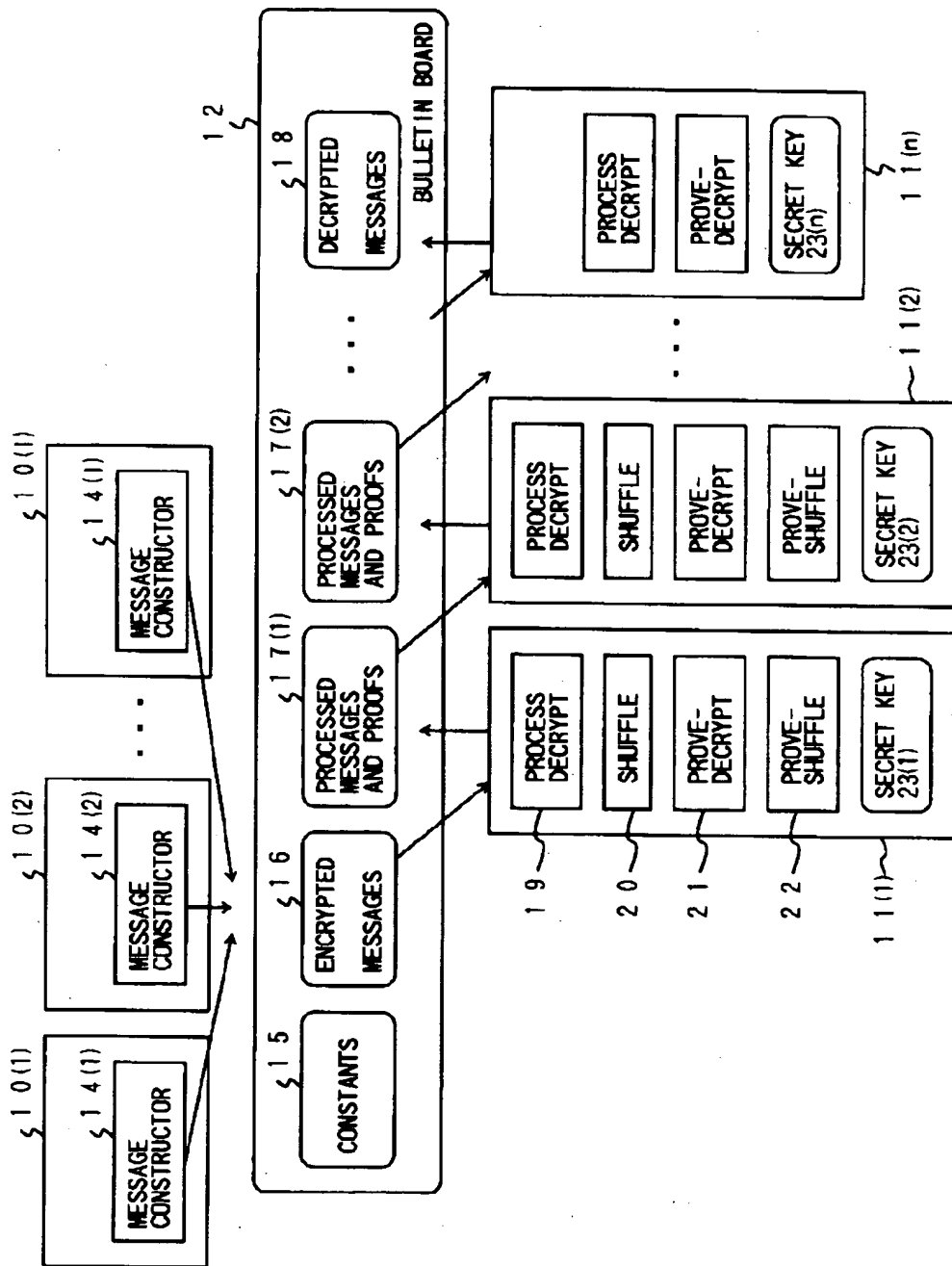


Fig.3

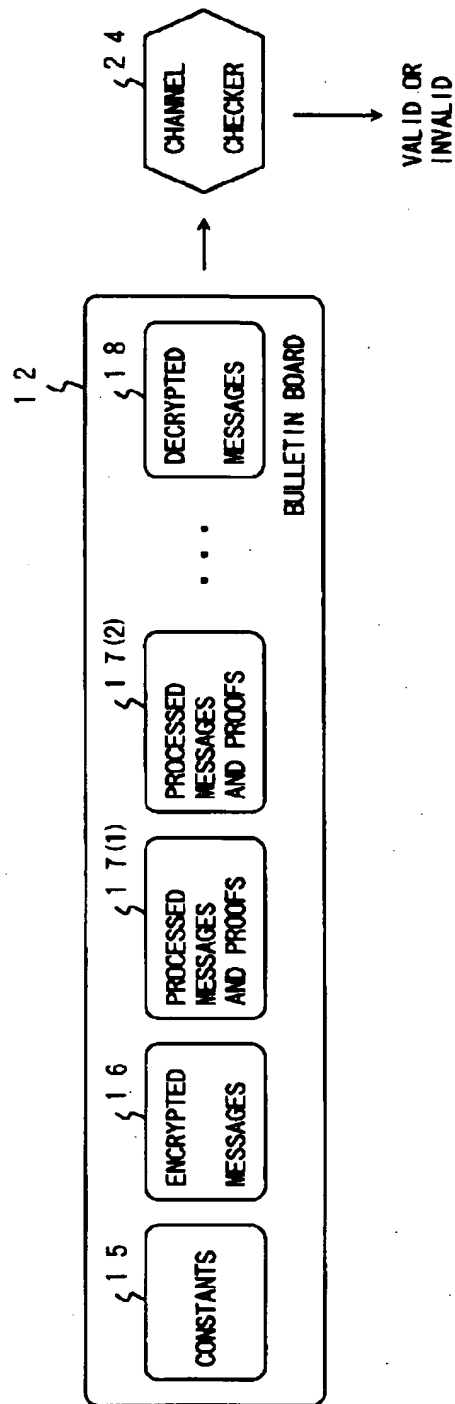
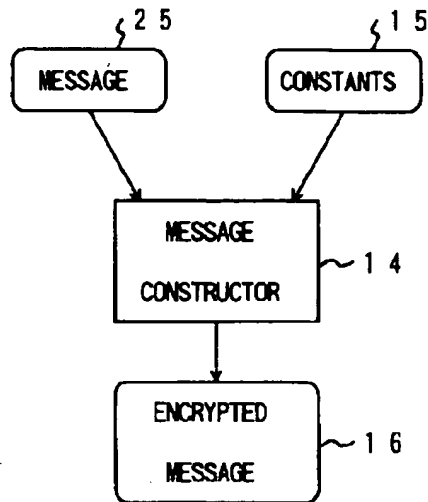




Fig.4



### 1. Abstract

A number-theoretic based algorithm provides for secure anonymous message transfer and electronic voting. A voter or sender may cast an encrypted vote or message that is processed through  $n$  centers in a manner which prevents fraud and authenticates the votes. Any interested party can verify that each vote has been properly counted. The invention can be realized by current-generation personal computers with access to an electronic bulletin board.

### 2. Representative Drawing

FIG. 1